AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Levent Sasmazel
Case: 501008-A-01-US (Sasmazel)
Serial No.: 10/043,589
Filing Date: January 10, 2002
Group: 2134
Examiner: Andrew L. Nalven

Title: Method and Apparatus for Secure Internet Protocol Communication in a Call Processing System

---

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

(1) Appeal Brief.

There is no additional fee due in conjunction with the response. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Avaya Inc. Deposit Account No. 50-1602** as required to correct the error.

Respectfully submitted,

Joseph B. Ryan

Date: August 29, 2006

Joseph B. Ryan
Reg. No. 37,922
Attorney for Applicant(s)
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Levent Sasmazel
Case: 501008-A-01-US (Sasmazel)
Serial No.: 10/043,589
Filing Date: January 10, 2002
Group: 2134
Examiner: Andrew L. Nalven

Title: Method and Apparatus for Secure Internet Protocol Communication in a Call Processing System

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant (hereinafter "Appellant") hereby appeals the final rejection dated February 7, 2006 of claims 1, 6, 7, 13, 18, 19 and 25 of the above-identified application.

REAL PARTY IN INTEREST

The present application is currently assigned to Avaya Inc. or a subsidiary thereof. Avaya Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

STATUS OF CLAIMS

The present application was filed on January 10, 2002, with claims 1-25. Claims 1-25 remain pending. Claims 1, 2, 8, 13, 14, 20 and 25 are the independent claims.

Each of claims 1, 6, 7, 13, 18, 19 and 25 stands rejected under 35 U.S.C. §103(a). Claims 2-5, 8-12, 14-17 and 20-24 are allowed. Claims 1, 6, 7, 13, 18, 19 and 25 are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for providing secure communications between two or more end units of a call processing system via a communication switch of the system, where each of the end units are coupled between the communication switch and one or more terminals of the system. An illustrative embodiment of the recited call processing system is shown as system 100 in FIG. 1, and includes a communication switch in the form of call complex 102. End units 110-1, 110-2, . . . 110-N are coupled between the call complex 102 and respective sets of terminals 112. More particularly, associated with each of the end units 110-*i*, $i = 1, 2, \ldots N$, is a set of terminals denoted Extension *i*01, Extension *i*02, . . . Extension *i*XX. These extensions correspond generally to terminal endpoints serviced by the call complex 102, e.g., the call complex 102 can direct incoming calls to and receive outgoing calls from these extensions in a conventional manner. See the specification at page 4, line 25, to page 5, line 3.

The recited method includes the step of storing, in a memory associated with the communication switch, a plurality of sets of session key lists including a set of session key lists for each of the end units. An example of one such set of session key lists stored for a given one of the end units 110-1 of system 100 is shown in FIG. 3 of the drawings. The end unit 110-1 is the end unit having Extension 101, Extension 102, . . . Extension 1XX associated therewith, as shown in FIG. 1, although it should be understood that similar sets of session key lists may be configured for each of the other end units 110. The set of session key lists for end unit 110-1 as shown in FIG. 3 includes session key lists denoted SKLST[0], SKLST[101], SKLST[102], . . . SKLST[1XX]. The session key list SKLST[0] includes only a single element as shown, while each of the other session key lists SKLST[101], SKLST[102], . . . SKLST[1XX], corresponding to respective terminals

Extension 101, Extension 102, . . . Extension 1XX, includes a table of M session keys, 312-1, 312-2, . . . 312-XX, respectively. See the specification at page 7, line 23, to page 8, line 16.

The recited method further includes the step of selecting as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch. As noted above, an example of a set of session key lists for end unit 110-1 is shown in FIG. 3, and a session key may be selected from one of the lists in the set of lists for end unit 110-1 for secure communications with another end unit. See the specification at, for example, page 11, lines 7-8 and 10-13.

The claim further recites that the end units have respective pluralities of terminals associated therewith, and that a given one of the end units is configured to provide an interface between its associated terminals and the communication switch. As noted previously, such an arrangement is shown in FIG. 1, where end units 110 have respective pluralities of terminals 112 associated therewith, and provide interfaces between their respective terminals 112 and the call complex 102. In addition, the claim recites that a given set of session key lists associated with the originating end unit comprises session key lists for respective terminals associated with that end unit, and that the given set of session key lists is generated in the originating end unit and transmitted from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch. As described above, an example of the set of session key lists associated with end unit 110-1 is shown in FIG. 3, and steps 400 and 406 of the flow diagram in FIG. 4 indicate that such a set of session key lists is generated by the end unit and sent to the communication switch. See the specification at page 9, lines 1-20.

Independent claim 13 is an apparatus claim, and recites a memory and processor configured to provide operations similar to those described above in the context of claim 1. An example of the recited apparatus may be call complex 102 as shown in FIG. 2, which includes memory 202 and processor 200. See the specification at page 6, lines 13-20.

Independent claim 25 is an article of manufacture claim, directed to a machine-readable storage medium storing one or more programs for use in a call processing system such as system 100 of FIG. 1. Such a machine-readable storage medium may comprise, for example, memory 202 in call complex 102 as shown in FIG. 2. See the specification at, for example, page 6, lines 21-26.

Advantageously, the claimed arrangements in the above-noted illustrative embodiments protect a call complex, end units and other elements of a call processing system from Internet protocol (IP) spoofing, denial of service, and other attacks, thereby facilitating secure and efficient implementation of IP communications within such a system. See the specification at, for example, page 3, lines 19-22, and page 18, lines 20-23.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 6, 7, 13, 18, 19 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0046534 (hereinafter "Alldredge") in view of U.S. Patent No. 6,148,404 (hereinafter "Yatsukawa").

ARGUMENT

§103(a) Rejection of Claims 1, 6, 7, 13, 18, 19 and 25

Claims 1, 13 and 25

A proper *prima facie* case of obviousness requires that the cited references when combined must "teach or suggest all the claim limitations," and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Appellant submits that the Examiner has failed to establish a proper *prima facie* case of obviousness in the present §103(a) rejection of claims 1, 13 and 25, in that the Alldredge and Yatsukawa references, even if assumed to be combinable, fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for combining the references or for modifying the reference teachings to reach the claimed invention. Further, even if it is assumed that

a proper *prima facie* case has been established, there are particular teachings in one or more of the references which controvert the obviousness argument put forth by the Examiner.

As indicated previously, each of independent claims 1, 13 and 25 recites an arrangement in which a given end unit provides an interface between an associated plurality of terminals and a communication switch, and specifies that a set of session key lists associated with an originating end unit comprises session key lists for respective terminals associated with that end unit. Each of these independent claims further specifies that a given set of session key lists is generated in the originating end unit and transmitted from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch.

It is also important to note that the claims call for storing a plurality of sets of session key lists including a set of session key lists for each of the end units. As noted previously herein, an example of one such set of session key lists stored for a given one of the end units 110-1 of system 100 is shown in FIG. 3 of the drawings. The end unit 110-1 is the end unit having Extension 101, Extension 102, . . . Extension 1XX associated therewith, as shown in FIG. 1, although it should be understood that similar sets of session key lists may be configured for each of the other end units 110. The set of session key lists for end unit 110-1 as shown in FIG. 3 includes session key lists denoted SKLST[0], SKLST[101], SKLST[102], . . . SKLST[1XX]. The session key list SKLST[0] includes only a single element as shown, while each of the other session key lists SKLST[101], SKLST[102], . . . SKLST[1XX], corresponding to respective terminals Extension 101, Extension 102, . . . Extension 1XX, includes a table of M session keys, 312-1, 312-2, . . . 312-XX, respectively. See the specification at page 7, line 23, to page 8, line 16.

Appellant initially notes that certain of the characterizations of Alldredge as proffered by the Examiner appear to be deficient. For example, as indicated above, the claims in question call for storing in a memory associated with a communication switch a plurality of sets of session key lists including a set of session key lists for each of the end units. The Examiner argues that such a plurality of sets of session key lists, with one set of session key lists for each end unit, and the end units providing an interface between the switch and respective terminals, is shown in paragraphs

[0024]-[0026], [0059] and [0067] of Alldredge. See the final Office Action at page 2, section 2. Appellant respectfully submits that this is a mischaracterization of the teachings of Alldredge. The relied-upon arrangements in Alldredge relate to first and second sequences of encryption key material, where the first sequence is "provided to an anonymous first user" and the second sequence is "provided to an encryption server." See Alldredge at paragraph [0023] and FIG. 1. The first and second sequences of encryption key material are "complementary sequences such that the encryption key material of the one sequence decrypts encrypted messages that have been encrypted with the other sequence," and may be "sequences of identical session keys." With reference to FIG. 2 of Alldredge and paragraph [0077], it is apparent that the first sequence of encryption key material is stored in a terminal of the system, namely, portable data storage device 25, which is illustratively shown as a portable computer. Thus, the first and second sequences relied upon by the Examiner do not constitute a plurality of sets of session key lists including a set of session key lists for each of the end units, where a given one of the end units provides an interface between the switch and a corresponding plurality of terminals.

In formulating the §103(a) rejection, the Examiner acknowledges that Alldredge fails to meet the above-noted limitations relating to generation of a set of session key lists in an end unit and the transmitting of the set of session key lists from the end unit to the switch, but argues that the deficiencies of Alldredge are overcome by the teachings in column 5, line 57, to column 6, line 28, of Yatsukawa. See the final Office Action at page 4, last two paragraphs, to page 5, first paragraph. The portions of the Yatsukawa reference relied upon by the Examiner provide as follows:

> FIG. 6 shows a sequence taken when the client A logs into a server B. The processing in FIG. 6 is divided into phases (2 and 3) for sharing a session key used for common-key enciphering (DES, IDEA and the like), and phases (4, 5 and 6) for performing authentication processing. The processing sequence is described below.
>
> 1 Client A sends a log-in request to server B.
>
> 2 Based on the log-in request, the server B sends the client A, a public key of the server B, random number and the like used for session-key sharing.

3 Client A generates a session key, enciphers the session key by using the public key of the server B and sends it to the server B. When the server B receives the enciphered session key, the session key is shared by the client A and server B. In the subsequent processing, all messages transferred between the client A and server B are enciphered by the session key and transmitted.

4 Client A sends a public key and user name of the client A to the server B.

5 The server B verifies that the public key and user name of the client A are registered, generates challenge data (random number) for authentication, enciphers the challenge data by using A's public key and sends it to the client A.

6 Client A calculates a hash value of the challenge data, and sends the calculated value to the server B as challenge-response data.

7 The server B compares the value of the challenge-response data received in step 6 with a hash value of the stored challenge data directed to the client A, and if they are the same value, the log-in request is granted to the client A, while if they are different, the log-in request is rejected.

An advantage of the SSH scheme is in that since the challenge data changes each time, "masquerading" by a third person is impossible even if the third person steals a message in the processing sequence 6. However, there is a disadvantage in that, if an administrator of the server B changes the client A's public key with ill intention, the administrator can "masquerade" as the client A.

Appellant respectfully submits that the foregoing passage fails to supplement the deficiencies of Alldredge as applied to the independent claims. For example, it fails to teach or suggest the claimed generation of a set of session key lists in an originating end unit and transmission of the set of session key lists from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch. In the above-cited passage from Yatsukawa, client A simply establishes a session key with server B and then participates in a challenge-response authentication protocol with that same server B. In an

arrangement of this type, there does not appear to be any need whatsoever for generation or transmission of sets of session key lists between entities A and B.

It is therefore believed that the collective teachings of Alldredge and Yatsukawa fail to meet the limitations of independent claims 1, 13 and 25, and fail to provide the associated advantages in terms of protecting a communication switch and end units from attacks while facilitating secure IP communications in a call processing system.

With regard to motivation to combine the references, the Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344.

The purported objective evidence of motivation to combine, provided by the Examiner at page 4, last paragraph, to page 5, first paragraph, of the final Office Action, appears to be conclusory in that it fails to indicate with sufficient specificity why or how one skilled in the art would combine Alldredge with Yatsukawa to reach the claimed invention. The Examiner relies primarily on the statement in column 6, lines 21-25, of Yatsukawa, which relates to the use of "challenge data" provided by server B to client A in the authentication protocol. However, the claimed invention relates to generation of a set of session key lists in an originating end unit and transmission of the set of session key lists from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch. It is believed that the relied-upon portion of Yatsukawa relating to use of challenge data in a challenge-response authentication protocol between two entities fails to motivate the proposed combination with Alldredge.

Appellant also notes that the session key referred to in Yatsukawa is established for use between client A and server B. However, the claims indicate that the session keys recited therein are for respective terminals associated with an end unit, and not session keys established between the

end unit itself and the communication switch. Yatsukawa would therefore seem to require that the recited originating end unit itself establish a session key with the communication switch, which is not what is claimed. Accordingly, the Yatsukawa disclosure actually seems to teach away from the claimed invention. Such a teaching away is believed to constitute evidence of non-obviousness sufficient to overcome any *prima facie* case that may have been established.

It should also be noted in this regard that the Alldredge reference similarly teaches away from the claimed invention, by teaching simple session key establishment between terminals of the system and an encryption server, without reference to end units that provide an interface between the terminals and a communication switch of a call processing system. Arrangements of this type are believed to suffer from one or more of the disadvantages noted by Appellant in the background portion of the specification.

Dependent claims 6, 7, 18 and 19 are believed allowable for at least the reasons identified above with regard to their respective independent claims, and are also believed to define separately-patentable subject matter as outlined below.

Claims 6 and 18

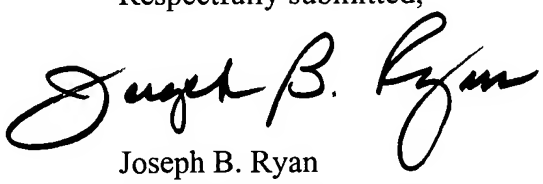
Dependent claims 6 and 18 further specify that the set of session key lists for a given one of the end units is supplied to the communication switch in encrypted form by that end unit as part of an authentication protocol carried out between that end unit and the communication switch. The Examiner argues that such an arrangement is met by the teachings in Alldredge at paragraph [0031], relating to a second sequence provided to an encryption server by a user. See the final Office Action at page 5, second paragraph. Appellant respectfully disagrees. There is no teaching or suggestion in the relied-upon portion of Alldredge to the effect that a set of session key lists is supplied from a given end unit to a switch in encrypted form. The passage in question simply indicates that the second sequence is "provided to" the encryption server. Accordingly, it is believed that the proposed combination of Alldredge and Yatsukawa fails to meet the particular limitations of dependent claims 6 and 18.

Claims 7 and 19

Dependent claims 7 and 19 further specify that a first session key element of the set of session key lists is utilizable for providing secure communications between the given one of the end units and the communication switch subsequent to completion of the authentication protocol. The Examiner argues that such an arrangement is met by the teachings in Alldredge at paragraph [0032], relating to interactions between a user and server 13. See the final Office Action at page 5, third paragraph. Appellant respectfully disagrees. This passage does not indicate that a first session key element of a set of session key lists is used subsequent to completion of an authentication protocol as recited. To the contrary, the passage relates to encryption of a message utilizing the first sequence. See paragraph [0033] of Alldredge. Accordingly, it is believed that the proposed combination of Alldredge and Yatsukawa fails to meet the particular limitations of dependent claims 7 and 19.

In view of the above, Appellant believes that claims 1, 6, 7, 13, 18, 19 and 25 are in condition for allowance, and respectfully requests the withdrawal of the §103(a) rejection.

Respectfully submitted,



Date: August 29, 2006

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. In a call processing system, a method for providing secure communications between two or more end units of the system via a communication switch of the system, each of the end units being coupled between the communication switch and one or more terminals of the system, the method comprising the steps of:

storing in a memory associated with the communication switch a plurality of sets of session key lists including a set of session key lists for each of the end units;

selecting as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch;

wherein the end units have respective pluralities of terminals associated therewith, a given one of the end units being configured to provide an interface between its associated terminals and the communication switch;

wherein the given set of session key lists associated with the originating end unit comprises session key lists for respective terminals associated with that end unit; and

wherein the given set of session key lists is generated in the originating end unit and transmitted from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch.

6. The method of claim 1 wherein the set of session key lists for a given one of the end units is supplied to the communication switch in encrypted form by that end unit as part of an authentication protocol carried out between that end unit and the communication switch.

7. The method of claim 1 wherein a first session key element of the set of session key lists is utilizable for providing secure communications between the given one of the end units and the communication switch subsequent to completion of the authentication protocol.

13. An apparatus for use in a call processing system for providing secure communications between two or more end units of the system via a communication switch of the system, each of the end units being coupled between the communication switch and one or more terminals of the system, the apparatus comprising:

a memory associated with the communication switch and operative to store a plurality of sets of session key lists including a set of session key lists for each of the end units; and

a processor coupled to the memory, the processor being operative to select as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch;

wherein the end units have respective pluralities of terminals associated therewith, a given one of the end units being configured to provide an interface between its associated terminals and the communication switch;

wherein the given set of session key lists associated with the originating end unit comprises session key lists for respective terminals associated with that end unit; and

wherein the given set of session key lists is generated in the originating end unit and transmitted from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch.

18. The apparatus of claim 13 wherein the set of session key lists for a given one of the end units is supplied to the communication switch in encrypted form by that end unit as part of an authentication protocol carried out between that end unit and the communication switch.

19. The apparatus of claim 13 wherein a first session key element of the set of session key lists is utilizable for providing secure communications between the given one of the end units and the communication switch subsequent to completion of the authentication protocol.

25. An article of manufacture comprising a machine-readable storage medium storing one or more programs for use in a call processing system for providing secure communications between two or more end units of the system via a communication switch of the system, each of the end units

being coupled between the communication switch and one or more terminals of the system, wherein the one or more programs when executed implement the steps of:

storing in a memory associated with the communication switch a plurality of sets of session key lists including a set of session key lists for each of the end units;

selecting as an end unit to end unit session key a session key from a session key list in a given one of the sets of session key lists associated with an originating end unit, the selected end unit to end unit session key being utilizable in providing secure communications between the originating end unit and at least one other end unit via the communication switch;

wherein the end units have respective pluralities of terminals associated therewith, a given one of the end units being configured to provide an interface between its associated terminals and the communication switch;

wherein the given set of session key lists associated with the originating end unit comprises session key lists for respective terminals associated with that end unit; and

wherein the given set of session key lists is generated in the originating end unit and transmitted from the originating end unit to the communication switch in conjunction with an authentication protocol carried out between the originating end unit and the communication switch.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None